UNIVERSITÀ DI PARMA
Dipartimento di Ingegneria e Architettura

Introduction

Luca Veltri

(mail.to: luca.veltri@unipr.it)

Course of Cybersecurity, 2022/2023

http://netsec.unipr.it/veltri

Security

- Making a system (a software, a computer, a network, etc.) secure, requires three types of security:
  - **physical security**
    - physically limit the access to the system
      - servers behind a locked door and only a privileged set of employees have access to it
      - use of cameras, card readers, and biometric locks
    - protection again information leakage
      - e.g. by shredding documents before they're thrown away
  - **technological security**
    - communication and data security
    - software security
      - application security
      - OS security
  - **good policies and practices**

Security Service

- Something that enhances the security of the systems and the information transfer
  - **aims to protect data, systems, user information**
  - **intended to counter security attacks**
- A processing or communication service that is provided by a system to give a specific kind of protection to system resources
  - **RFC 4949 , "Internet Security Glossary"**
    - https://tools.ietf.org/html/rfc4949
- Makes use of one or more security mechanisms to provide the service
- Replicates functions normally associated with physical objects/documents
  - **e.g. signatures, dates, proof of reception, notarization, recording, etc.**

Security Services (cont.)

- Some security services:
  - **Confidentiality**
  - **Data integrity and message authentication (authenticity)**
  - **Peer entity authentication (identification)**
  - **Authorization and access control**
  - **System integrity and availability**
  - **Accountability and non-repudiation**
  - **Anonymity**

Security Services (cont.)

- Confidentiality
  - **protects data against unauthorized disclosure**
    - It is the property that information is not made available to unauthorized entities
    - related to
      - data
        - » data confidentiality
      - entities involved in the communication
        - » anonymity

Security Services (cont.)

- Data integrity and message authentication
  - **data integrity**
    - the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner
      - protects against unauthorized changes to data by ensuring that changes to data are detectable
      - in general it can only detect a change
  - **data origin authentication**
    - provides for the corroboration of the source of a data unit
      - this service verifies the identity of a system entity that is claimed to be the original source of received data
    - usually provided together with data integrity → message authentication
  - **message authentication (authenticity)**
    - both data integrity and origin authentication
    - in general, authenticity implies integrity but integrity doesn't imply authenticity

Security Services (cont.)

- Identification (peer entity authentication)
  - **verification of the identity of a peer entity**
    - before the establishment of a communication or the access to a resource/service

- Authorization and access control
  - **authorization**
    - verification of the permission to access a resource or system
      - manage access rights/privileges
  - **access control**
    - ability to limit and control the access to a systems
      - protection of system resources against unauthorized access

Security Services (cont.)

- System integrity and availability
  - **system integrity**
    - the quality that a system has when it can perform its intended function
      - protects system resources against unauthorized change, loss, or destruction
  - **availability**
    - protects a system to ensure its availability
      - addresses the security concerns raised by denial-of-service (DoS) attacks

Security Services (cont.)

- Accountability and non-repudiation
  - **accountability**
    - property of a system or system resource that ensures that the actions of an entity may be traced uniquely to that entity
  - **audit**
    - service that records information needed to establish accountability
  - **non-repudiation**
    - provides protection against false denial of an action
      - it provides evidence that can be stored and later presented to a third party
    - in case of a communication, it prevents either sender or receiver from denying a transmitted message
      - the receiver can prove that the sender in fact sent the message
        - » non-repudiation with proof of origin
      - the sender can prove that the receiver in fact received the message
        - » non-repudiation with proof of receipt

Security Services (cont.)

- Anonymity
  - **The condition of an identity being unknown or concealed**
    - An application may want to maintain anonymity of users or other system entities, perhaps to preserve their privacy
    - When a two (or more) parties interact without letting the possible observers detect such relation
      - who is talking with whom

Security Mechanisms

- Security services are provided by means of different security functions/ mechanisms
  - **they can be included in appropriate communication layer**

- Examples of security mechanisms are:
  - **enciphering**
  - **authentication exchange**
  - **data integrity check**
  - **digital signature**
  - **notarization (third-party authentication)**
  - **access control**
  - **traffic padding**
  - **routing control**
  - **etc.**

Relationship Between Security Services and Mechanisms

	Mechanism							
Service	**Enciph-erment**	**Digital signature**	**Access control**	**Data integrity**	**Authenti-cation exchange**	**Traffic padding**	**Routing control**	**Notari-zation**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Classification of Security Attacks

- **Passive attacks** (eavesdropping on, or monitoring of transmissions):
  - **Interception (snooping)**
    - obtain message contents (attacks confidentiality)
  - **Traffic analysis**
    - monitor traffic flows (attacks confidentiality)
- **Active attacks** (modification of data stream):
  - **Spoofing**
    - fabrication of messages with a fake source entity (attacks authenticity)
  - **Tampering**
    - modify of message content (insert, cancel, modify data) (attacks integrity)
  - **Replay/Reflection**
    - replay previous messages to/from the same of different entity (attacks authenticity)
  - **Repudiation**
    - deny having sent or received a message (attacks Non-reputation)
  - **Denial of Service (DOS)**
    - Interruption of a network or application service (attacks availability)